Norma de Gestão de Vulnerabilidades dos Ativos de Informação da UFV

O GESTOR DE SEGURANÇA DA INFORMAÇÃO DA UNIVERSIDADE FEDERAL DE VIÇOSA (UFV), NA CONDIÇÃO DE COORDENADOR DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO DA UFV, no uso de suas atribuições legais e regimentais, resolve aprovar a Norma que estabelece diretrizes e procedimentos para a gestão de vulnerabilidades dos ativos de informação da Universidade Federal de Viçosa (UFV):

CAPÍTULO I: INTRODUÇÃO

Art. 1° - Os termos e definições relacionados a esta norma podem ser encontrados na Política de Segurança da Informação e Comunicações (POSIC) da UFV, conforme estabelecido na Resolução CONSU-UFV Nº 16/2019, e no glossário de segurança da informação do Governo Federal, segundo a Portaria GSI/PR Nº 93, de 18 de outubro de 2021.

Art. 2° Referências Legais e Normativas:

- Política de Segurança da Informação e Comunicações da Universidade Federal de Viçosa (UFV):
- Modelo de Política de Gerenciamento de Vulnerabilidades da Secretaria de Governo Digital (SGD);
- ABNT NBR ISO/IEC 27001:2022;
- NIST Framework for Improving Critical Infrastructure Cybersecurity, Versão 1.1 (2018).
- CIS Controls v8;

Art. 3° Escopo:

Esta norma se aplica a todos os usuários de ativos de informação da Universidade Federal de Viçosa (UFV).

Art. 4º: Estabelecimento de um Processo de Gestão de Vulnerabilidades dos Ativos de Informação da UFV (PGV-UFV):

§ 1º Este artigo define a estrutura e as responsabilidades para a gestão de vulnerabilidades dos ativos de informação da Universidade Federal de Viçosa (UFV), com o envolvimento do Comitê de Segurança da Informação e Comunicações (CSIC-UFV), da Diretoria de Tecnologia da Informação (DTI), e da Equipe de Tratamento e Resposta a Incidentes Cibernéticos da UFV (ETIR-UFV).

I. Estratégia e Governança (CSIC):

a. Desenvolver e revisar periodicamente uma estratégia de gestão de vulnerabilidades alinhada com os objetivos institucionais da UFV.

b. Realizar auditorias semestrais para avaliar a aderência da política e dos processos às normas de segurança.

II. Identificação e Análise de Vulnerabilidades (ETIR-UFV):

a. Coordenar varreduras periódicas em todos os ativos de informação para identificar vulnerabilidades.

b. Analisar as vulnerabilidades identificadas e fornecer um relatório detalhado à DTI após cada varredura.

III. Medidas de Remediação e Mitigação (ETIR-UFV):

a. Coordenar o tratamento das vulnerabilidades críticas identificadas de forma prioritária.

b. Também estabelecer planos de tratamento para vulnerabilidades de média e baixa criticidade.

IV. Atualizações e Gerenciamento de Atualizações (“Patches”) e correções de falhas de vulnerabilidade (DTI / STI):

a. Coordenar a implementação de atualizações (“patches”) de segurança críticas após o lançamento das mesmas.

b. Para atualizações menos críticas, considerar prazos mais dilatados para a mitigação das mesmas.

V. Treinamento e Conscientização (CSIC / ETIR-UFV):

a. Realizar sessões de treinamento para as equipes envolvidas no programa de gestão de vulnerabilidades (PGV-UFV).

b. Promover campanhas de conscientização periódicas para a comunidade universitária sobre a importância da segurança dos ativos de informação.

VI. Monitoramento e Avaliação (ETIR-UFV e DTI):

a. Implementar monitoramento contínuo para a detecção de novas vulnerabilidades, com relatórios periódicos à DTI.

b. A CSIC deve realizar avaliações periódicas acerca da eficácia do PGV-UFV e propor ajustes conforme necessário.

Art. 5° - Quando aplicável, todas as atividades referentes ao PGV-UFV deverão ser registradas e documentadas.

Art. 6° - Os casos omissos desta norma serão resolvidos pelo CSIC-UFV, sempre em consonância com os princípios gerais de segurança da informação, a missão e os valores da Universidade Federal de Viçosa, bem como a legislação aplicável.

CAPÍTULO II: POLÍTICA DE GESTÃO DE VULNERABILIDADES

Art. 7º: Processo de Gerenciamento de Vulnerabilidades (PGV-UFV):

§ 1º Este artigo define os procedimentos e a metodologia para a efetiva gestão de vulnerabilidades dos ativos de informação da Universidade Federal de Viçosa (UFV), envolvendo diversas unidades e responsabilidades dentro da instituição.

I. Criação, Implementação e Manutenção do PGV-UFV:

a. A CSIC será responsável por criar e manter o PGV-UFV, garantindo que esteja sempre alinhado com as melhores práticas e requisitos regulamentares.

b. O PGV-UFV deve ser revisado e atualizado periodicamente, ou conforme necessário, para refletir mudanças no ambiente tecnológico ou nas prioridades institucionais.

II. Mecanismos para Obtenção de Informações sobre Vulnerabilidades:

a. A Equipe de Tratamento e Resposta a Incidentes Cibernéticos da UFV (ETIR-UFV) deverá estabelecer mecanismos para a coleta contínua de informações sobre novas vulnerabilidades, utilizando fontes confiáveis e atualizadas.

b. Este mecanismo deve incluir a subscrição em feeds de vulnerabilidade, grupos de segurança, e bases de dados especializadas.

c. ETIR-UFV poderá se relacionar com as demais equipes de prevenção, tratamento e resposta a incidentes cibernéticos da Administração Pública Federal; com o Centro de Tratamento de Incidentes de Redes do Governo - CTIR.gov, com o Centro de Atendimento a Incidentes de Segurança da Rede Nacional de Pesquisa (CAIS-RNP), ou equivalente; com os órgãos, entidades e empresas, públicas ou privadas, que tenham relacionamentos com a UFV para o intercâmbio de informações; e com a Secretaria de Governo Digital (SGD).

III. Gestão de Vulnerabilidades em Diversos Ativos de Informação:

a. A ETIR-UFV, em colaboração com a DTI / STI, deve garantir que a gestão de vulnerabilidades abranja todos os ativos de informação da UFV, incluindo redes, sistemas operacionais, aplicações web e móveis.

IV. Atividades de Suporte ao PGV-UFV:

a. A CSIC e a DTI / STI deverão fornecer suporte contínuo ao PGV-UFV, incluindo recursos, treinamento e ferramentas necessárias para a execução eficaz das atividades de gestão de vulnerabilidades.

V. Funções e Responsabilidades no PGV-UFV:

a. As funções e responsabilidades de todos os envolvidos no PGV-UFV devem ser claramente definidas e documentadas pelo CSIC, assegurando que todas as partes compreendam suas tarefas e responsabilidades.

VI. Atualizações de Software e Fontes de Informação sobre Vulnerabilidades:

a. A ETIR será responsável pela coordenação das ações que envolvam atualizações de software e patches de segurança, garantindo que sejam aplicadas de maneira tempestiva e eficaz.

b. A ETIR-UFV deve garantir que as equipes técnicas mantenham-se informadas sobre as últimas vulnerabilidades e atualizações (“patches”) disponíveis.

VII. Métricas de Gerenciamento de Vulnerabilidades:

a.Tanto a CSIC como a ETIR-UFV deverão estabelecer e monitorar métricas chave (Key Performance Indicators - KPIs) para avaliar a eficácia do PGV-UFV, incluindo, mas não se limitando a, tempo de resposta a vulnerabilidades e eficácia de remediação.

b. A CSIC deverá definir métricas adicionais para monitorar e avaliar o desempenho do PGV-UFV, garantindo que esteja em conformidade com as políticas e estratégias de segurança da informação da UFV.

CAPÍTULO III: IMPLEMENTAÇÃO E EXECUÇÃO DO PGV-UFV

Art. 8º: Detecção de Vulnerabilidades nos Ativos de Informação da UFV

§ 1º Este artigo estabelece as diretrizes para a detecção de vulnerabilidades nos ativos de informação da Universidade Federal de Viçosa (UFV), com a participação ativa da Equipe de Tratamento e Resposta a Incidentes Cibernéticos da UFV (ETIR-UFV) e da Diretoria de Tecnologia da Informação (DTI), e do Serviço de Tecnologia da Informação (STI).

I. Ações Relacionadas à Detecção de Vulnerabilidades:

a. A ETIR-UFV deverá definir, coordenar e executar ações sistemáticas para a identificação proativa de vulnerabilidades nos ativos de informação da UFV.

b. Estas ações incluem a análise contínua do ambiente de TI para identificar potenciais vulnerabilidades e ameaças.

II. Configuração e Ajuste de Ferramentas de Detecção:

a. A ETIR-UFV será responsável por configurar e manter atualizadas as ferramentas de detecção de vulnerabilidades, garantindo a cobertura abrangente de todos os ativos de informação relevantes.

b. As configurações devem ser revisadas e ajustadas regularmente para assegurar a detecção eficiente e precisa de vulnerabilidades.

III. Frequência e Tipos de Testes de Segurança:

a. A ETIR-UFV, em conjunto com a equipe técnica, deverão realizar testes de segurança de forma periódica.

b. Os testes de segurança devem incluir tanto varreduras automatizadas quanto inspeções manuais, para garantir uma avaliação abrangente das vulnerabilidades.

IV. Varreduras de Vulnerabilidades e Testes de Penetração (“Pentests”):

a. A ETIR-UFV deverá conduzir varreduras de vulnerabilidades regulares, utilizando ferramentas atualizadas e métodos eficazes para identificar vulnerabilidades em todos os ativos de informação da UFV.

b. Além disso, a ETIR-UFV deverá realizar testes de penetração (“pentests”) de forma periódica, para avaliar a resiliência dos sistemas e redes da UFV contra ataques cibernéticos.

OBS: A execução eficaz das atividades de detecção de vulnerabilidades é crucial para a identificação precoce de riscos potenciais, permitindo a implementação de medidas de remediação apropriadas de forma eficaz.

CAPÍTULO IV: AVALIAÇÃO E REMEDIAÇÃO

Art. 9º: Elaboração de Relatórios de Vulnerabilidade

§ 1º Este artigo estabelece a obrigatoriedade e os procedimentos para a elaboração de relatórios de vulnerabilidade na Universidade Federal de Viçosa (UFV), enfatizando a importância da documentação detalhada e precisa das vulnerabilidades detectadas nos ativos de informação.

I. Processo de Elaboração de Relatórios:

a. A Equipe de Tratamento e Resposta a Incidentes Cibernéticos da UFV (ETIR-UFV) será responsável por elaborar relatórios detalhados das vulnerabilidades detectadas.

b. Estes relatórios devem incluir informações como a natureza da vulnerabilidade, os ativos afetados, a severidade e o potencial impacto sobre a UFV.

II. Análise e Classificação de Vulnerabilidades:

a. Cada vulnerabilidade identificada deve ser analisada e classificada pela ETIR-UFV com base em sua severidade e impacto potencial.

b. Esta classificação é crucial para determinar a prioridade de remediação e para o planejamento de medidas de mitigação adequadas.

III. Comunicação de Vulnerabilidades:

a. Os relatórios de vulnerabilidade devem ser comunicados ao CSIC, à DTI / STI, e às partes relevantes dentro da UFV.

b. O CSIC será responsável por garantir que as informações contidas nos relatórios sejam utilizadas para informar decisões estratégicas e operacionais relacionadas à segurança da informação.

IV. Documentação e Armazenamento de Relatórios:

a. Todos os relatórios de vulnerabilidades devem ser devidamente documentados e armazenados em um repositório central seguro, acessível apenas por pessoal autorizado.

b. Esta documentação deve ser mantida por um período mínimo estabelecido em Lei, para fins de auditoria e análise histórica.

OBS: A elaboração regular e precisa de relatórios de vulnerabilidade é fundamental para o monitoramento contínuo das ameaças à segurança da informação da UFV e para a melhoria contínua das práticas de segurança cibernética.

Art. 10º: Priorização e Correção de Vulnerabilidades

§ 1º Este artigo delineia as diretrizes para a priorização e correção de vulnerabilidades identificadas nos ativos de informação da Universidade Federal de Viçosa (UFV), enfatizando a necessidade de respostas rápidas e eficazes para mitigar riscos à segurança da informação.

I. Procedimentos de Aceitação de Risco e Exceções:

a. Em casos onde a correção imediata de uma vulnerabilidade não for viável, a ETIR-UFV deve documentar e submeter para a CSIC um processo de aceitação de risco, detalhando a justificativa, os controles compensatórios em vigor e um plano de ação para mitigação futura.

b. A aceitação de risco deve ser aprovada pelo CSIC e revisada periodicamente para assegurar que os riscos sejam minimizados.

c. As exceções devem ser monitoradas continuamente até que as vulnerabilidades sejam efetivamente corrigidas ou mitigadas.

II. Monitoramento e Reavaliação de Vulnerabilidades:

a. A ETIR-UFV deve monitorar continuamente o status das vulnerabilidades, assegurando que as ações de correção sejam implementadas conforme planejado.

b. As vulnerabilidades devem ser reavaliadas periodicamente para garantir que as correções aplicadas sejam efetivas e para identificar quaisquer novas exposições decorrentes das correções.

III. Relatório de Progresso e Avaliação de Eficácia:

a. A ETIR-UFV deve elaborar relatórios periódicos sobre o progresso das ações de correção de vulnerabilidades, incluindo informações sobre vulnerabilidades corrigidas, pendentes e exceções.

b. Estes relatórios devem ser apresentados à CSIC para avaliação da eficácia do processo de correção de vulnerabilidades e para a tomada de decisões informadas sobre as estratégias de segurança da informação.

OBS: A abordagem sistemática para a priorização e correção de vulnerabilidades é essencial para a manutenção da integridade, confidencialidade e disponibilidade dos ativos de informação da UFV, contribuindo para a resiliência organizacional contra ameaças cibernéticas.

CAPÍTULO V: COMUNICAÇÃO E REGISTROS DE LOGS

Art. 11º: Comunicação da Ocorrência de Vulnerabilidades

§ 1º Este artigo estabelece os procedimentos para a comunicação eficaz de vulnerabilidades identificadas nos ativos de informação da Universidade Federal de Viçosa (UFV), visando assegurar a transparência e a rápida disseminação de informações críticas para a segurança da informação.

I. Procedimentos de Comunicação de Vulnerabilidades:

a. A Equipe de Tratamento e Resposta a Incidentes Cibernéticos da UFV (ETIR-UFV) é responsável pela comunicação imediata de vulnerabilidades críticas à CSIC e outras partes interessadas.

b. A comunicação deve incluir detalhes sobre a natureza da vulnerabilidade, os ativos afetados, e as ações recomendadas ou em andamento para a remediação.

II. Disseminação de Informações de Vulnerabilidade:

a. A CSIC deve estabelecer canais de comunicação efetivos para disseminar informações sobre vulnerabilidades a todas as unidades relevantes dentro da UFV.

b. As informações devem ser divulgadas de forma clara e compreensível, evitando termos técnicos desnecessários e enfatizando as ações necessárias.

III. Comunicação com Usuários e Partes Externas:

a. Quando apropriado, a CSIC, e/ou ETIR, devem comunicar vulnerabilidades relevantes aos usuários finais e a terceiros afetados, orientando sobre medidas preventivas ou de mitigação.

b. Estas comunicações devem ser coordenadas pela CSIC para garantir consistência e clareza nas mensagens.

IV. Registros de Comunicação:

a. Todas as comunicações relacionadas a vulnerabilidades devem ser documentadas e arquivadas para referência futura e análise.

b. Esta documentação deve incluir datas, conteúdo da comunicação, destinatários e feedback recebido, se houver.

V. Revisão e Melhoria do Processo de Comunicação:

a. A CSIC deve revisar periodicamente os procedimentos de comunicação de vulnerabilidades para garantir que sejam eficientes e eficazes.

b. Feedback de usuários e partes interessadas deve ser utilizado para melhorar continuamente os processos de comunicação.

OBS: A comunicação eficiente e oportuna de vulnerabilidades é um aspecto crítico do gerenciamento de segurança da informação, permitindo respostas rápidas e minimizando o impacto potencial de vulnerabilidades na UFV.

Art. 12º: Registros de Logs e Análise

§ 1º A gestão de Logs na UFV será tratada em norma específica.

CAPÍTULO VI: SERVIÇOS EM NUVEM E DE TERCEIROS

Art. 13º: Responsabilidades em Serviços de Nuvem e de Terceiros

I. Avaliação e Seleção de Fornecedores:

a. A UFV, através da DTI / STI, deve conduzir avaliações detalhadas de potenciais fornecedores de serviços em nuvem e terceiros, enfatizando a segurança de dados e a gestão de vulnerabilidades.

b. Critérios de seleção devem incluir a conformidade com as normas de segurança da informação, histórico de segurança, e capacidades de resposta a incidentes.

II. Acordos de Nível de Serviço (SLAs):

a. Os SLAs devem incluir cláusulas específicas sobre gestão de vulnerabilidades, incluindo a frequência de atualizações de segurança e respostas a incidentes.

b. Os SLAs devem ser revisados periodicamente para garantir que permaneçam alinhados com as necessidades e políticas de segurança da UFV.

III. Monitoramento e Avaliação Contínua:

a. A UFV deve monitorar o desempenho de segurança dos serviços em nuvem e terceiros, utilizando métricas e indicadores-chave de desempenho.

b. Avaliações de segurança periódicas e auditorias devem ser realizadas para verificar a conformidade com os acordos estabelecidos e identificar possíveis vulnerabilidades.

IV. Gestão de Incidentes e Resposta a Vulnerabilidades:

a. Procedimentos claros de resposta a incidentes devem ser estabelecidos com fornecedores, incluindo notificação imediata de quaisquer vulnerabilidades ou brechas de segurança.

b. Planos de ação devem ser implementados rapidamente para mitigar vulnerabilidades detectadas em serviços de nuvem ou fornecidos por terceiros.

V. Treinamento e Conscientização:

a. Programas de conscientização devem ser implementados para manter a segurança da informação como uma prioridade constante na utilização de serviços externos.

VI. Revisão e Melhoria Contínua:

a. A UFV deve revisar e atualizar continuamente suas estratégias e procedimentos relacionados a serviços em nuvem e de terceiros, visando aprimorar a gestão de vulnerabilidades.

b. Feedback e lições aprendidas devem ser incorporados para melhorar continuamente a segurança e a eficácia dos serviços utilizados.

OBS: A gestão eficaz de vulnerabilidades em serviços de nuvem e de terceiros é crucial para proteger os ativos de informação da UFV contra ameaças cibernéticas. Este artigo visa estabelecer um quadro robusto de responsabilidades e procedimentos para garantir que esses serviços sejam utilizados de forma segura e alinhados com as políticas de segurança da UFV.